

Binary Tree

تعلم كيف تحمي نفسك على الانترنت من خلال شرح لأهم الثغرات
و الحيل و الأدوات التي يستخدمها الهاكرز في عملياتهم

مكتبة الطـــارق الاكترونية

Designer by : aLTar3q
Designer by : aLTar3q

بسم الله الرحمن الرحيم

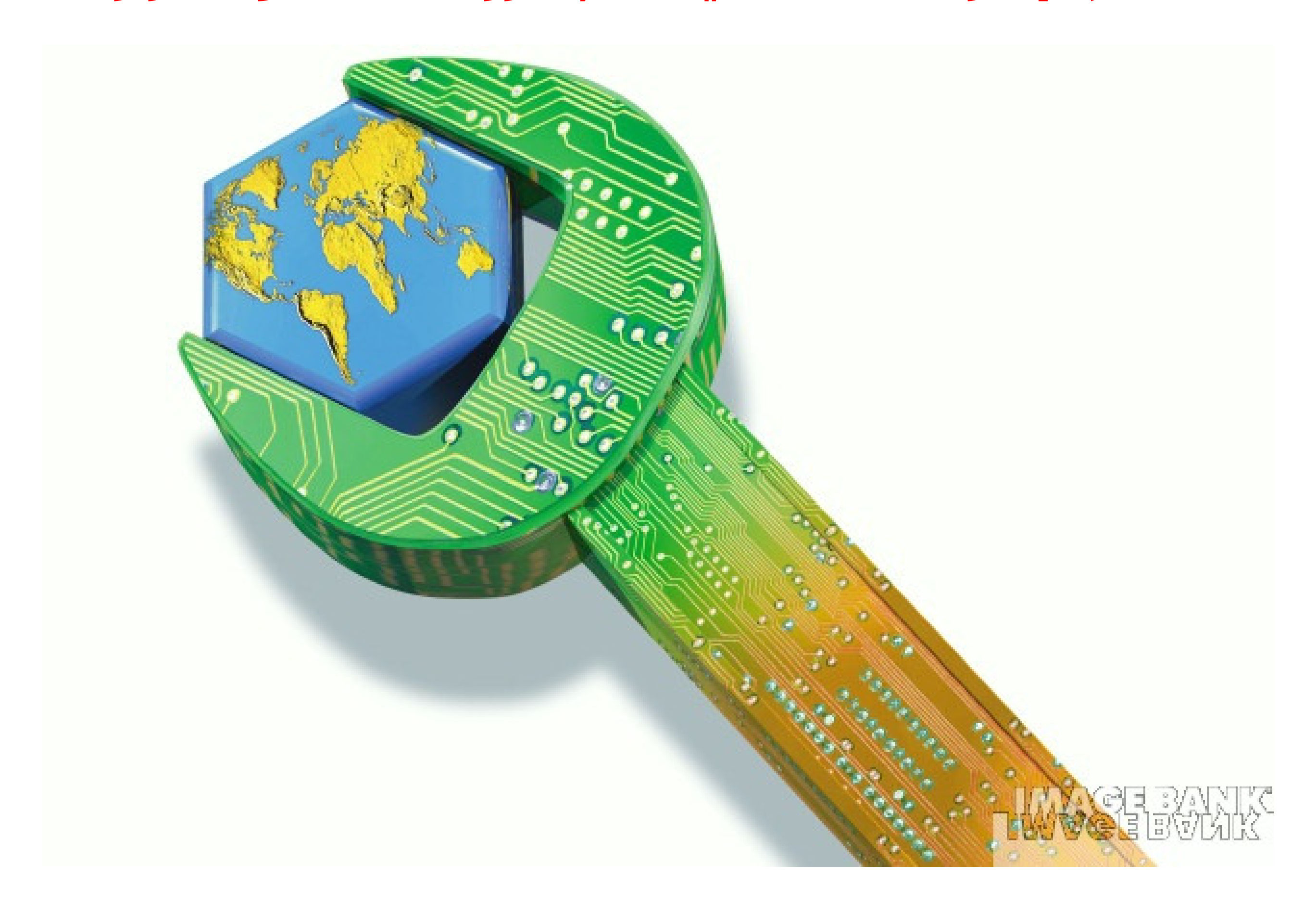
Binary Tree

موقع قاعة المطورين

http://www.devhall.com

&&&&&&&&&&&&&&&&&&&&&&

عالم الإنترنت السفلي : الهاكرز .. خفايا و أسرار



لست هنا بصدد كتابة مقالة تشرح لك كيف تخترق موقع ، أو كيف تخترق جهاز ضحية ما ، أو كيف تستولي على بريد إلكتروني ، ولكن سأضع بين يدي القارئ الكريم الخطوط العريضة لأهم الثغرات ، الحيل ، الأساليب ، و الأدوات التي يستخدمها الهاكرز في عملياتهم.

أعترف لك عزيزي القارئ بأنني ترددت كثيراً قبل كتابة هذه المقالة ، ترددت لأن هذه المقالة فعلا ستكون سلاح ذو حدين ، سلاح بيد المبرمج و المطور و مستخدمي الحاسب عموما لكي يعرفوا تماما حجم المخاطر المحدقه بهم و يضعوا في حسبانهم كل ما سيقرأونه في هذا المقالة من حيل و خدع و أساليب قد يستخدمها أحد الهاكرز تجاههم .

وهي سلاح أيضاً بيد من يمتلك نوايا سيئه و خبيثه و يريد فقط من يدله على بعض الأساليب و الحيل ليكون قد وضعه قدمه على أول الطريق في مجال تعلم و إحتراف الإختراق. لذا أستأذنك عزيزي القارئ بعدم الخوض في بعض التفاصيل ، فسأكتفي بشرح بعض الأمور شرحاً واضحا يوصل المعلومة بشكل كامل ولكن قدر المستطاع لن يستفيد أي شخص من هذه المعلومه لإستخدامها أغراض سيئه (أعلم ان ذلك سيكون صعب ، ولكني سأحاول :)

ملاحظة : فليعذرني القارئ الكريم إن كانت هناك مصطلحات عربية غير مفهومه ، فقد إستخدمت مصطلحات التعريب القياسية في بعض أرجاء هذه المقالة ، و أحيانا أخرى أضطررت لتعريب بعض المصطلحات بنفسي لعدم معرفتي بتعريب قياسي لهذا المصطلح!

من هو الهاكر ؟

تعارف الناس على إطلاق مصطلح هاكر على الشخص الذي يقوم بإختراق التطبيقات أو الأجهزة أو الشبكات ، أو يقوم بالتحايل للحصول على معلومات حساسة (مثل بطاقتك الإئتمانية ، حسابك البنكي ، معلومات بطاقة التأمين ... الخ) .

في هذه المقالة سنستخدم هذا المصطلح للدلالة على هذا المفهوم ، ولكن لكي نضع الأمور في نصابها ، أود أن أوضح أن هذا المصطلح بهذا المفهوم خاطئ ، نعم هو كذلك ، مصطلح هاكر يطلق أساساً على الشخص الذي يمتلك قدرات خارقة في مجال البرمجة و التطوير و لديه موهبة عالية في التفكير المنطقي و الرياضي و يستطيع حل أي مشكلة برمجية مهما كانت معقدة بسرعة فائقة و بالطريقة الأمثل .

نذكر على سبيل المثال ، بيل جيتس مؤسس شركة مايكروسوفت و كبير المهندسين فيها ، يصنف هذا الرجل علميا ضمن فئة الهاكرز في المفهوم الصحيح للكلمة .

حيث يمتلك هذا الرجل قدرات برمجية مذهلة ، نذكر منها على سبيل المثال برمجته للغة BASIC في 8 أسابيع فقط ! علما أنه قام بتطوير هذه اللغة لصالح جهاز جديد حينها يطلق عليه ATARI لم يكن بيل جيتس يمتلك هذا الجهاز .

و أعتمد فقط في برمجته للغة على الدليل الورقي لمعمارية الجهاز ، و المذهل أنه قام بعرض اللغة على أحد الشركات و قام بتشغيل برنامج مفسر اللغة Interpreter) لأول مرة بدون أي عملية تجربة سابقة (لأنه لم يكن يمتلك الجهاز الذي صنع من أجله هذه اللغة) ، و كانت النتيجة برنامج يتنفذ بدون ظهور أي خطأ !

هذا أمر يعتبر في عرف المبرمجين أمر خرافي ، لأن اي برنامج مهما كان صغير لا بد و أن تظهر فيه (غالبا (أخطاء كثيرة وقت البرمجة و بعد ذلك ، فما بالك حينما يكون البرنامج هو مفسر للغة برمجة جديدة !

حيث تعتبر برمجة المفسرات Compilers or Interpreter من أعلى و أعقد مراتب البرمجة. هذا مثال على شخص يطلق عليه مسمى هاكر بالمفهوم الأساسي لمعنى الكلمة .عموما سنستخدم كلمة هاكر في هذه المقالة للدلالة على المعنى الدارج والمنتشر وهو الشخص الذي يستخدم قدراته التقنية لأغراض خبيثه و غير شرعية.

الهاكرز و جهازك الشخصي

عادة تكون أولى خطوات الهاكر المبتدئ هي محاولة إختراق الأجهزة الشخصية ، عملية إختراق الأجهزة الشخصية عملية سهلة نسبياً ، لذا تكون هي الخطوة الأولى في رحلة ذلك الهاكر (إن صح تسميته هاكر) .

على الرغم من إنتشار برامج الحماية في الفترة الأخيرة و إزدياد الوعي لدى مستخدمي الإنترنت ، الى أنه ما زال هناك من تنطلي عليه حيل بعض هؤلاء الهاكرز ليتمكنوا من السيطرة على جهازه .

بشكل عام لن يتمكن أي هاكر من إختراق جهازك الا اذا كان الجهاز مصاب ببرنامج يفتح باب خلفي Backdoor يسهل دخول الهاكر إلى الجهاز ، هذه البرامج التي تفتح أبواب خلفية في جهازك تسمى أحصنة طروادة Trojan Horses و وظيفتها بالتحديد فتح منفذ Port في جهازك يستخدمه الهاكر عن طريق برنامج إختراق جاهز و معد مسبقاً يحتوي على كافة الخصائص و الخدمات التي تخدم أغراض الهاكر و تسهل عليه مهامه .

على سبيل المثال ، سيتمكن الهاكر من قراءة كل حرف تكتبه على لوحة المفاتيح أثناء إتصالك بالإنترنت ، أيضا سيكون بوسعه سحب كافة كلمات المرور الخزنه في الذاكرة ، سيستطيع أيضا فتح ملفاتك ، قراءة رسائلك ، و مشاهدتك عبر الكاميرا ، بل سيستطيع مشاركتك في المواقع التي تتصفحها و المحادثات التي تجريها!



صورة لبرنامج سب سفن الشهير في مجال إختراق الأجهزة الشخصية

تنطلق شرارة المشكلة عندما تقوم بفتح تطبيق أو ملف لا تعرف مصدره سواء كان هذا الملف مرسل اليك عن طريق البريد الإلكتروني أو قمت بنفسك بتحميله على جهازك من أحد المواقع أو أحد الأقراص التي حصلت عليها .

بعض ملفات التجسس (أحصنة طروادة) تكون مضمنه ضمن خلفية شاشة جميله أو لعبة صغيرة أو برنامج تطبيقي آخر مشهور ! عند تشغيلك لهذا التطبيق تكون ببساطة فتحت باب خلفياً Backdoor للهاكرز و سيكون بمقدوره إختراق جهازك و العبث فيه ، كل ما سيحتاجه معرفة رقم الأي بي الخاص بك وقت إتصالك وهذه المعلومة من السهل جداً الحصول عليها بحيل و اساليب لن أسهب في ذكرها خوفاً من أن تستغل إستغلالاً سيئ!

النصيحة : لا تفتح أي ملف أو برنامج يصلك عبر البريد الإلكتروني من شخص غير معروف ، أو تجده في موقع غير مشهور ، و تأكد دائما من تحديث مضاد الفايروسات وملفات التجسس في جهازك بشكل دوري (كل أسبوع على الأكثر) .

كما تأكد من تركيب جدار حماية Firewall جيد مثل برنامج زون ألارم Zone Alarm لحماية منافذ الجهاز و إغلاق المنافذ المشهورة التي تستخدمها بعض تطبيقات الإختراق المنتشرة بين يدي المبتدئين من الهاكرز!

الهاكرز و مواقع الويب

هذا الفرع قد يكون متشعب جدا ، و يصعب فعلاً تغطيته في مقالة أو حتى عشرة مقالات لأن هناك العديد من الحالات و الأساليب التي يمكن نصنفها تحت مسمى إختراق المواقع ، فمن الممكن مناقشة هذا الموضوع من جهة مطوري الموقع ، أو من جهة أصحاب و ملاك المواقع ، و نظرا لأهمية الناحيتين ، فسأناقش الموضوع من هذين الجانبين بشكل مختصر و غير مخل بإذن الله.

أصحاب المواقع .. و الإختراق

أنت تمتلك موقعا ، اذا بياناتك متاحة لملايين البشر ، يفصلها عنهم فقط زوج من البيانات (إسم مستخدم و كلمة مرور) ، الحصول على زوج البيانات هذا هو مهمة ذلك الهاكر ، و أحيانا يكون غير مضطر لمعرفة هذه البيانات ، ببساطة يمكن للهاكر إستغلال أحد ثغرات نظام التشغيل في سيرفر الشركة المستضيفة لموقعك ، أو إستغلال ثغرة من ثغرات التطبيقات التي تقوم بتركيبها في موقعك مثل المنتديات أوالمجلات الإلكترونية أو أي تطبيق تقوم بتركيبه .

معرفة هذه الثغرات ليس بالأمر الصعب ، يكفي أن يقوم أحد الهاكرز بالإشتراك بالرسائل الإخبارية التي تأتي من شركة VB المنتجه لبرنامج المنتديات الشهير و التي تبلغ عن أي ثغرة تكتشف في النظام ليذهب ذلك الهاكر مسرعا يبحث عن منتدى لم يقم بالترقية بعد و يستغل تلك الثغرة فيه!

نصائح أمنية لأصحاب المواقع

- تأكد من شركة الإستضافة التي تتعامل معها من إصدارة نظام التشغيل و لوحات التحكم لديهم و قم بالبحث عن هذه الإصدارات و تأكد ما اذا كانت تحتوي على ثغرات خطيرة أو لا.

- إستخدم في موقعك فقط البرمجيات التي تحتاج اليها فكرة الموقع فقط، اذا كنت لست بحاجة ماسة إلى سجل زوار ، فلا تضعه ، اذا لم تكن بحاجه لمحرك بحث داخلي ، فلا تضع.

- ركب دائما أحدث النسخ من البرمجيات التي تستخدمها في الموقع ، سواء المنتديات أو المجلات الإلكترونية.

- لا تبالغ في تركيب الإضافات الغير أساسية على التطبيقات ، هذه الإضافات) تعرف أيضاً بالهاكات) تساهم كثيرا في فتح ثغرات في موقعك ، وذلك لأنها صممت و برمجت من قبل هواة ولم تبرمج من قبل الشركة المنتجه لنفس البرنامج (على سبيل المثال الهاكات المستخدمة في برامج المنتديات هي في الغالب سبب إختراق معظم المنتديات ، و العجيب أننا نرى بعض أصحاب المنتديات يتفاخرون بعدد الهاكات التي يستخدمونها و التي هي في الحقيقة أبواب خلفية مفتوحة لإختراق مواقعهم :(!!

- أحرص دائما على تتبع أخبار البرمجيات التي تستخدمها في موقعك و تأكد من أنك تقوم بالترقية في حالة وجود ثغرة خطيرة وليس فقط في حالة وجود ميزة جديدة في البرنامج ، كثرة الترقيات المبالغ فيها قد تسبب لك المشاكل ايضاً.

- لا تثق في أحد ، لا تعطي بيانات موقعك لأي جهة غير رسمية ، قد تحتاج الى تركيب برنامج أو تصليح مشكلة في موقعك ، تأكد من أنك تتعامل مع مواقع و جهات على درجة عالية من الموثوقية وليس مع بعض الهواة في المنتديات.

- راقب سجلات الدخول Logs في موقعك متى ما أحسست أن هناك أمر مريب يجري سجلات الدخول كنز من المعلومات يجدر بك إستغلاله للأغراض الأمنية أو الإحصائية

- حدد صلاحيات المشاركات في موقعك ، اذا كنت تمتلك منتدى فلا تسمح للأعضاء بإضافة وسوم HTML أو جافا سكريبت ، أحدهم قد يسرق ملفات الكوكيز الخاصة بك بهذه الطريقة!!

إذا لم تكن قادرا على تولي تنفيذ هذه النصائح الأمنية بنفسك ، فيمكنك إستئجار جهة خارجية لتقوم بذلك عنك ، أحد أفضل المواقع العربية في هذا المجال هو موقع الحلول الأمنية و المتخصص بتقديم الخدمات الأمنية لأصحاب المواقع .

الهاكرز يا مطوري تطبيقات الويب!

هل سمعت عن XSS ؟
هل تعرف ما هي حقن لغة الإستعلام SQL Injection
هل قرأت عن إقتحام الجلسات Session Hijacking
حسنا ، هل قرأت عن الـCRLF Injection ،
ماذا عن الـ Directory Traversal ،
و ماذا عن التلاعب بالمتغيرات؟ Parameters Manipulation

حسناً ... هذه الأسئلة ستعطي إنطباع عن أن الموضوع متشعب جداً ، لم أذكر هنا الا أهم و أشهر أنواع المشاكل و الثغرات التي يستغلها الهاكرز لتدمير التطبيقات التي تبرمجها ، و اذا كنت لم تسمع بواحد أو أكثر من هذه المصطلحات ، فأنت في خطر!

بما أن هذا الجزء من المقالة يهم مطوري المواقع أكثر من غيرهم ، فلن أسهب كثيراً بشرح هذه المصطلحات و طريقة عملها ، أتوقع أنك كمطور قادر على البحث بنفسك عن تفاصيل هذه المصطلحات و معرفة ما هو المعني البرمجي لها بالضبط ، عموما ، سأذكر رؤوس أقلام عن هذه المصطلحات للمهتمين بتنمية ثقافتهم الأمنية في شتى المجالات.

الـ Cross Site Scripting

يطلق عليها إختصاراً xss وليس CSS تميزاً لها عن صفحات الأنماط المتعددة Cascading Style Sheet، بإختصار هي نوع من الهجمات التخريبية على تطبيقك يحدث عندما يتمكن أحدهم من إدخال بيانات مختلطة مع بعض الأوامر في نماذج صفحات موقعك ينتج عن ذلك تشويه شكل صفحة موقعك أو إظهار رسائل خطأ متكررة عند زيارة الصفحة التي تم تخريبها، أو سرقة بعض البيانات الحساسة من الزوار أو صاحب الموقع نفسه !

تنتج هذه المشكلة نتيجه عدم فحصك لمدخلات الزوار في النماذج و سماحك لهم بإدخال وسوم HTML أو Java Script في نماذج الموقع مما يجعلهم قادرين على تلويث صفحات موقعك بشيفرات ليست جزء من شيفرة تطبيقك الذي كتبته ! يمكن للهاكر أيضاً العبث في المتغيرات التي يمررها تطبيقك عن طريق عناوين URL و إضافة أجزاء اليها تجعله قادر على السيطرة جزئيا أو كلياً على تطبيقك ، أو على الأقل تشويه شكل التطبيق ، لعلك تتذكر عزيزي القارئ الثغرة التي كان مصاب بها نظام بريد الـ Hotmailقبل سنتين تقريبا ، و التي كانت تسمح للهاكر بقراءة صندوق البريد الوارد للضحية ، تلك الثغرة كانت تصنف تحت الـ! XSS

الـ SQL Injection

تحت هذه النقطة سأحيلك عزيزي القارئ إلى مقالة كتبتها سابقا عن هـذا الموضوع بالتحديد ، المقالة هي: الـ SQL Injection سلاح الدمار الشامل ضد تطبيقات الويب ، أتمنى أن تستمتع بقراءة تلك المقالة ، الموضوع خطير و يستحق مقالة منفردة.

إقتحام الجلساتSession Hijacking

إقتحام الجلسات هي عملية السيطرة على جلسة المستخدم Session الذي يقوم بإستخدام النظام ، عملية إقتحام الجلسه تلزم أن يقوم الهاكر بإلتقاط رقم الجلسة Session ID، أو توليد إجباري لها Brute Force أو إعادة توليد للرقم Reverse Engineering، قد يبدو المفهوم صعب حالياً لذا سأسترسل بشرحه أكثر.

من المعروف أن هناك نوعين من الجلسات الجلسات الدائمة Persistent وهي التي يتم من أجلها تعريف ملفات الإرتباط (الكوكيز) و حفظها في جهاز المستخدم لكي يتعرف عليه النظام عند عودته في أي وقت مرة أخرى ! .

النوع الثاني هي الجلسات الغير دائمة non-Persistent وهي التي تنتهي بمجرد إغلاق المستخدم للمتصفح ، في كلا النوعين يتم تعريف رقم جلسة Session ID للمستخدم ، رقم الجلسه هذا يستخدم لمعرفة متغيرات المستخدم الذي يرسلها أو يستقبلها خلال جلسته على النظام ، هذا الرقم ينشئ عادة بشكل إفتراضي من لغة البرمجة التي تستخدمها من خلال رقم أي بي المستخدم وقت الجلسه يدمج معها بعض المتغيرات الأخرى .

بعض المبرمجين يكتفي بتوليد هذا الرقم بشكل إفتراضي دون أن يسعى لتشفيره أو إضافة المزيد من العوامل عليه لجعل عملية التوليد الإجباري أو إعادة التوليد له صعبة ، و هنا تكمن المشكلة حيث يقوم الهاكر بمحاولة توليد رقم الجلسه بمعرفة بعض المعطيات اللحظية و يرسلها عن طريق HTTP Request إلى النظام الذي يقرأ رقم الجلسه و يقارنه برقم الجلسه الموجود لديه في الذاكرة ، فإذا تطابق ، فهذا يعني من وجهة نظر النظام أن الهاكر هو المستخدم الحقيقي .

و يمنحه بذلك حق الوصول لمنطقة المستخدم الخاصة (حسابه البنكي على سبيل المثال) !! ، الجدير بالذكر أن هجمات الـ xss يمكن أن تستخدم للإستيلاء على الجلسات و ذلك عن طريق تمرير كود جافا سكربت للنظام يقوم بقراءة رقم جلسة المستخدم و ارسال هذا الرقم للهاكر!

نصائح لتجنب هذا النوع من المشاكل

- حاول تشفير رقم الجلسه و تعقيدها قدر المستطاع

- إستخدم الـ SSL لتشفير كافة البيانات الحساسة المرسلة و المستقبلة من و إلى نظامك

- برمجياً قم بإنهاء أي جلسه يمضي عليها وقت كافي تقدر بأن المستخدم خلالها قد إنتهى فعلاً من عمله خلالها أو انه قد ترك شاشة النظام مفتوحة و لم يعد يستخدمها

- حصن نظامك ضد هجمات الـXSS

الـ CRLF Injection

مصطلح CRLF هو إختصار لـ Carriage Return , Line Feed ، الـ CR هو رمز الأسكي 13و الـ LF هو رمز الأسكي 10 ، هذان الرمزان يستخدمها الويندوز عند الضغط على زر Enter أي للنزول إلى سطر جديد .

نظام لينكس يستخدم فقط الرمز LF ، بإختصار هذا النوع من الهجمات ليس خطير للغاية ، أقصى ما يمكن للهاكر فعله من خلال هذه النوعية من الثغرات هو تشويه شكل الصفحة ، بالتأكيد هذه المشكلة قد تكون حساسه حسب نوعية التطبيق الذي تقوم ببرمجته.

هذا النوع من الهجوم يكون أيضا بسبب عدم فحص مدخلات المستخدم (تماما كالـ SQL Injectionو الـ xss) ، تأكد من أن المستخدم لا يدخل علامة \n\r في المدخلات (الا في الأماكن التي يسمح بها للمستخدم بإستخدام هذه الرموز للنزول الى سطر جديد)

مثلا في نص الموضوع الذي يكتبه العضو في المنتدى يجب أن تسمح له بإستخدام زر Enter الذي يتحول عند الضغط عليه إلى \n\r ولكن غير مرئية ! ، ولكن في عنوان الموضوع سيكون السماح للمستخدم بإدخال رمز CRLF مشكلة كبيرة!!

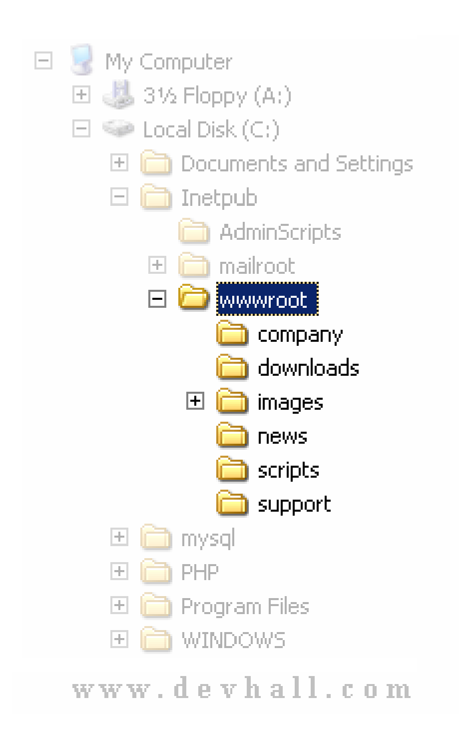
التجول في المجلداتDirectory Traversal

هذا النوع من الهجمات خطر فعلا ، لن أبالغ اذا قلت انه اخطر أنواع الهجمات على الإطلاق ، ما يخفف من وطئته هو أنه صعب التطبيق لأن التطبيقات التي يمكن إستغلال هذا النوع من الثغرات فيها محدودة جداً ، ولكن هذا لا يمنع من أنه خطر و خطر جداً !

فكرة هذا النوع من الهجمات ببساطة هو أن يتمكن الهاكر من الخروج عن نطاق مجلد الجذر للموقع Root directory إلى مجلدات أخرى تعلو المجلد الجذري في المستوى ، دعني أضرب مثال لتوضيح الصورة ، في سيرفرات الويندوز التي تعمل بالـ IIS يكون مجلد الجذر للموقع عادة هو:

C:\Inetpub\wwwroot

وهذا المجلد هو الذي تتواجد فيه ملفات موقعك ، و بالتالي فإن الزوار سيتمكنون فقط من تصفح الملفات الموجودة في هذا المجلد و المجلدات الفرعية الموجود بداخله ، ومنها على سبيل المثال مجلد news ، الصورة في الأسفل تعطيك إنطباع عن التسلسل الشجري للمجلدات التي سأضرب مثال عليها.



الأن تخيل لو أن لديك عنوان في تطبيقك الذي برمجته بهذا الشكل

http://www.yoursite.com/news/show.aspx?view=file.html

العنوان يقوم بإستدعاء الملف file.html و عرضه للمستخدم ، الملف file.html يفترض أن يكون موجود في نفس مجلد news ، إفترض الأن لو أن الهاكر قام بالتلاعب في العنوان و كتبه بهذا الشكل:

http://www.yoursite.com/news/show.aspx?view=../../../../../Windows/system.ini

مصيبة ... لقد تمكن من مشاهدة ملف الـ System.ini !! ماذا لو أن التطبيق الذي برمجته يسمح بالتعديل على محتوى الملف ، سيتمكن الهاكر حينها من التعديل على ملف< System.ini

مما يعني تحكم كامل في موقعك من نظام التشغيل ، ليس فقط في الموقع بل و في كامل السيرفر المستضيف لموقعك ! الأسوء من ذلك تخيل لو ان نظامك يسمح بتشغيل بعض التطبيقات على الموقع عن طريق أوامر الشل (يفترض أن لا تبرمج هذا النوع من التطبيقات !) ، لو تمكن الهاكر من الخروج من المجلد الجذري كما في المثال السابق ، قد يتمكن من الوصول الى سطر الأوامر الرئيسي و تنفيذ أمر Format للسيرفر بأكمله!!

هذا النوع من الهجمات يمكن أن يحل بطريقتين ، و برأيي يجب أن تستخدم الطريقتان لحل المشكلة:

1 - من خلال الشيفرة التي تكتبها ، تأكد من فحصك لكافة المدخلات و المتغيرات الممررة إلى النظام ، تأكد من أنها تقع ضمن النطاق المسموح به

2 - من خلال إعدادات السيرفر الذي تمتلكه (أو تمتلكه الشركة المستضيفه لموقعك (يمكن ضبط هذه الإعدادت بحيث يتم منع أي طلب للوصول الى أي ملف خارج المجلد الجذري للموقع نفسه ، قم بفحص السيرفر بنفسك مبدئيا عن طريق السماح من خلال الشيفرة بأن تفتح ملف يقع خارج المجلد الجذري لموقعك ، إن إستطعت ذلك فهذا يعني أن إعدادات السيرفر المستضيف لموقعك غير آمنة و يجب أن تعدل بحيث يمنع السيرفر نفسه طلب أي ملف خارج نطاق المجلد الرئيسي ، أطلب من الشركة المستضيفة لموقعك تعديل ذلك ، و بدورك عدل الشيفرة كما ذكرنا في النقطة رقم 1 لمزيد من الحماية.

التلاعب بالمتغيرات Parameters Manipulation

أحد أشهر حيل الهاكر للوصول الى فهم كامل عن طريقة تعاملك مع المتغيرات الممرره الى النظام الذي قمت ببرمجته ، يتم ذلك عن طريق التلاعب بالمتغيرات الممرره إلى العنوان URL و تغيير قيمها أو إرسال قيم مخالفة لنوعية المتغير نفسه ، بحيث يستطيع الهاكر معرفة رسائل الخطأ التي تصدر من النظام حينها ، هذه الرسائل ستساعد الهاكر على فهم أكبر لتركيب النظام لديك .

أيضا قد يستخدم الهاكر طريقة التلاعب بالمتغيرات لتمرير متغيرات جلسه Session عن طريق العنوان مباشرة و ليس من خلال المتصفح نفسه بالـ HTTP Request ، في لغة البرمجة التي تستخدمها يفترض أن يكون هناك طريقة لمعرفة ما اذا كان متغير الجلسه هذا ممرر عن طريق الطلب HTTP Request من المتصفح نفسه ، أو من العنوان! URL كمثال أخر على هذا النوع من الهجمات ، نماذج صفحات الويب التي تقوم بتصميمها ليقوم الزائر بتعبئتها ، إما لغرض المراسلة أو التسجيل في الموقع أو شراء سلعة ... الخ ، يسهل على الهاكر قراءة أسماء عناصر النموذج .

هذه الأسماء بالتأكيد ستستخدمها أنت كمتغيرات في البرنامج الذي قمت ببرمجته ، إنطلاقا من هذه المعلومة يستطيع الهاكر إستخدام النموذج (أو صنع نموذج مشابه) مع تعديل قيم بعض الحقول لإحداث أثر ما على موقعك ، لكي أوضح المسألة ، دعني أذكر لك هذه القصة .

موقع التسوق الخاص بشبكة ياهوو Yahoo Shopping ، كان يستخدم طريقة محددة لتمرير سعر السلعة إلى صفحة الدفع ، فعند إختيارك للسلعة و تعبئته لنموذج بيانات الشحن ، يكون سعر السلعة أو السلع التي أخترتها موجود في نفس نموذج الشحن ولكن في حقل مخفي Hidden لا يظهر للزوار و لكنه موجود في شيفرة HTML ، قام أحد الهاكر حينها بتعديل شيفرة الـ HTML و قلل من سعر السلعة التي أرادها إلى دولار واحد ، و من ثم قام بتمرير الطلب بشكل طبيعي إلى صفحة الدفع ، التي حسمت السعر (دولار واحد) من بطاقته الإئتمانية و ظهر لمسؤولي الشحن أن هذا الرجل قد تمت عملية إستخلاص المبلغ من بطاقته بنجاح و أنه يستحق الشحن للسلع التي طلبها !!

الجميل في الأمر ان المشكلة أكتشفت فوراً و مصادفةً من أحد مسؤولي أمن المعلومات في أحد الشركات العالمية و الذي قام بتنبيه ياهوو حينها لتراجع سجلات المدفوعات لديها خوفا من أن تكون هذه الثغرة أستغلت بكثرة حيث وجدت أنها أستغلت فقط لمرة واحده!

حسنا أخي المطور ، أعتقد انني إستطعت من خلال هذه النقاط المختصرة تنبيهك إلى خطر محدق قد يسبب في ضياع جهدك في التطوير و التصميم بسبب أخطأ قد تبدو تافهه ، ولكنها تكلف الكثير أحيانا !! أعتقد أنني يجب أن افرد مقالة كاملة عن كل نوع من أنواع هذه الثغرات ، أعدك عزيزي القارئ أنني سأفكر في هذا الأمر بشكل جدي (:

رسائل الإحتيال Phishing Scam

سمي عام 2004 بعام رسائل الإحتيال Phishing Scam ، و أعتقد ان عام 2005 كان له نصيب أكبر كذلك ، رسائل الإحتيال ببساطة هي رسائل تصلك على بريدك الإلكتروني ، يدعي فيها مرسلوها أموراً يهدفون منها الى تحقيق مكسب مادي أو معنوي .

و أحيانا قليله لغرض التسلية فقط ، على سبيل المثال ، ظهرت قبل بضعة أشهر في المملكة العربية السعودية رسالة بريد إلكتروني أرسلت إلى عدد كبير جدا من المستخدمين .

تظهر هذه الرسالة للوهلة الأولى بأنها مرسلة من بنك سامبا ، حيث تطلب منك الرسالة ضرورة تحديث بياناتك البنكية عن طريق رابط موجود في نص الرسالة ، هذا الرابط يقودك إلى موقع مطابق في التصميم لموقع سامبا يطلب منك المحتال من خلاله إدخال بياناتك (إسم المستخدم و كلمة المرور و معلومة إضافية هي رقم بطاقة الأحوال !).

هذا مثال على أحد رسائل الإحتيال التي ظهرت في المملكة العربية السعودية ، و هذا النوع من الرسائل يظهر بشكل يومي في أمريكا و أوروبا . و فيما يلي أسرد لك عزيزي القارئ مجموعة من أشهر أنواع رسائل الإحتيال:

1 - رسائل تطلب منك إدخال بياناتك البنكية على أساس انها مرسلة من البنك الذي تتعامل معه.

2 - رسائل تطلب تسجيل معلوماتك الشخصية لأنك ربحت جائزة كبيرة!

3 - رسائل تدعي انها من موقع البريد الإلكتروني (هوتميل مثلاً) ، تطلب منك إعادة إدخال كلمة المرور!

4 - رسائل تطلب منك إدخال معلومات حساسة و تدعي بأنها من خلال هذه المعلومات ستقرأ مستقبلك أو تخبرك مدى توافقك مع شريك حياتك ... ، في الحقيقة هذه المعلومات طلبها صديق لك يريد معرفة اسرار حياتك:(

5 - رسائل تدعي بأنها شركات لتشغيل الأموال في تجارة العملات و تدعي بأنها تملك برنامج مخصص لتبادل العملات العالمية!

هناك العديد من أنواع الرسائل التي قد يخترعها أي شخص لأغراض التحايل ، لا تثق باي رسالة تطلب منك أي معلومة شخصية ، مهما بدت لك هذه المعلومة تافهه ، و مهما كان شكل الرسالة يوحي بأن مرسلها جهة موثوقة تعرفها جيدا ، حتى ولو رأيت أن عنوان البريد المرسله من هذه الرسالة هو عنوان بريد جهة رسميه ، فلا تثق بذلك بتاتا ، من السهل جدا أن أرسل لك رسالة تظهر لك بأن مرسلها هو العنوان : bush@whitehouse.gov ، فهل أنا الرئيس جورج بوش ؟

الرسائل المضلله Hoax Email

هذا النوع من الرسائل لا يسبب غالباً أخطار كبيرة ، ولكنه مزعج ، و أحيانا مضحك !

هذه الرسائل تحتوي عادة على تحذيرات كاذبة من فايروس ليس له وجود و إنما ترسل هذه الرسالة لغرض إثارة الذعر ، أو تسبيب أضرار في أحيان كثيرة ، إنتشار هذه الرسائل على النطاق العربي محدود جداً و كان آخرها رسالة مضحكة تحذر بأن الملف jdbgmgr.exe الموجود في نظام التشغيل ويندوز كملف أساسي من ملفات النظام هو فايروس يستهدف العرب دون غيرهم و أن مرسله شخص يهودي يقصد إستهداف المسلمين و العرب !!

طبعا هذه الشائعة إنتشرت في رسالة Hoax قبل حوالي سنتين باللغة الإنجليزية (لم يروج حينها أن صاحب الفايروس يهودي يستهدف المسلمين !) ، يبدو أن صاحبنا مبتدع النسخة العربية من هذه الرسالة مغرم بنظرية المؤامرة ! لمعرفة معلومات أكثر عن الرسائل المضلله و قائمه بأخر الرسائل المضلله التي تظهر على الساحة راجع هذا الرابط : http://www.symantec.com/avcenter/hoax.html

كلمة أخيرة

من خلال هذه المقالة حاولت تسليط الضوء على عالم الهاكرز و أشهر الحيل و الثغرات التي يستخدمها الهاكرز ، و على الرغم من تشعب الموضوع و كثرة فروعه ، الا انني حاولت أن أطرق معظم الأبواب أحيانا بأسلوب تقني بحت ، و أحيانا بأسلوب عام يتمكن من فهمه جميع مستخدمي الحاسب الآلي ، أعلم أن هناك العديد من المشاكل و الثغرات لم أتطرق لها ، منها ما يتعلق بعمليات التنصت على الشبكات Sniffing و منها ما يتعلق بعمليات الإدعاء Spoofing و منها ما يتعلق بهجمات الحرمان من الخدمة DOS أو جمع المعلومات التحليلية بغرض التخطيط لعملية الإختراق الفردي أو الجماعي ... ، عدم تطرقي لهذه المواضيع كان لسببين ، أولا بسبب شدة تخصصها لدرجة أظن معها بأن المقالة ستفقد جاذبيتها و بساطتها ، و السبب الثاني هو أن هذه المواضيع هي عناوين عريضة جدا يمكن أن نؤلف بها كتبا وليس مقالات ولا أريد أن أضع عناوين غير موضحه بشكل كافي لكي لا أدع القارئ مشتت و قد يخرج من قراءة هذه المقالة بإنطباع سلبي!

أتمنى أن أكون قد وفقت في طرح الموضوع بشكل سليم و وافي ، و أرغب بسماع تعليقاتكم الكريمة التي بالتأكيد ستزيدني حماس على مواصلة كتابة سلسلة كاملة عن هذا المجال ، مجال أمن المعلومات.

ملاحظة هامة : لك مطلق الحرية عزيزي القارئ بنقل هذه المقالة إلى أي منتدى أو أي موقع آخر ، ولكن نرجو الإشارة برابط مباشر إلى مصدر المقالة وليس فقط الإكتفاء بذكر انها منقولة ! ، هذه المقالة كلفت من الوقت و الجهد ما الله به عليم ، لذا ساهم معنا في حفظ حقوق كاتب المقالة بالإشارة الواضحة لمصدر المقالة